PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2002-140239**
(43)Date of publication of application : **17.05.2002**

(51)Int.Cl. **G06F 13/00**
G06F 12/00
G06F 15/00

(21)Application number : **2001-236093**
(22)Date of filing : **03.08.2001**

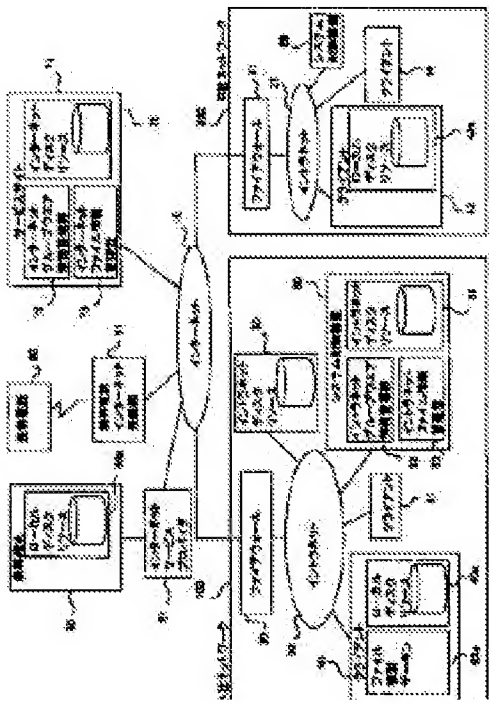
(71)Applicant : **MIZUNO MASAHIRO**
(72)Inventor : **MIZUNO MASAHIRO**
SUZUKI KAZUNARI

(30)Priority

Priority number	Priority date	Priority country
2000247446	**17.08.2000**	**JP**
2000 227025	**23.08.2000**	**US**

(54) INFORMATION MANAGEMENT SYSTEM, INFORMATION MANAGEMENT METHOD AND SYSTEM CONTROLLER

(57)Abstract:
PROBLEM TO BE SOLVED: To construct an information management system allowing a seamless access to information from the inside and outside of an intranet where conventionally information transmission between the Internet and the intranet has not been able to pass a system having high level security provided with a fire wall or the like.
SOLUTION: A system controller 60 for managing groupware information and files is provided on the intranet 30. A service site 70 is provided on the Internet 10. File duplicating daemons 63c are provided in each client 40 and 41. The file duplicating daemons 63c transfer files of data on the client 40 to disk resources 50, 61, and 71 on the intranet or the Internet in coordination with the system controller 60. The system controller 60 synchronizes the groupware information in coordination with the service site 70. In such manner, information can be seamlessly accessed from inside and outside the intranet.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号
特開2002－140239
（P2002－140239A）
(43)公開日　平成14年５月17日(2002.5.17)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード(参考)
Ｇ０６Ｆ　13/00	３５１	Ｇ０６Ｆ　13/00	３５１Ｚ	５Ｂ０８２
12/00	５３３	12/00	５３３Ｊ	５Ｂ０８５
	５４６		５４６Ａ	５Ｂ０８９
15/00	３１０	15/00	３１０Ｕ	

審査請求　未請求　請求項の数９　ＯＬ　（全 19 頁）

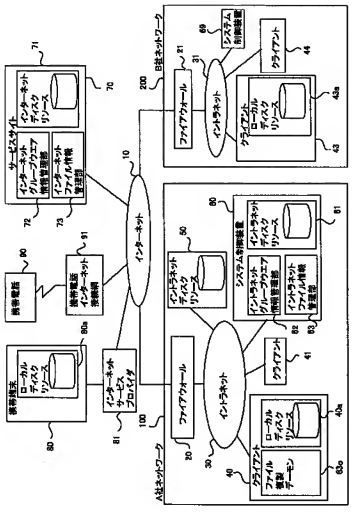
(21)出願番号　特願2001－236093(P2001－236093)
(22)出願日　平成13年８月３日(2001.8.3)
(31)優先権主張番号　６０／２２７０２５
(32)優先日　平成12年８月23日(2000.8.23)
(33)優先権主張国　米国（ＵＳ）
(31)優先権主張番号　特願2000－247446(P2000－247446)
(32)優先日　平成12年８月17日(2000.8.17)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　500388442
水野　正博
アメリカ合衆国　95008　カルフォルニア州　キャンベル　ソブラトドライブ　381
(72)発明者　水野　正博
アメリカ合衆国　95008　カルフォルニア州　キャンベル　ソブラトドライブ　381
(72)発明者　鈴木　一成
アメリカ合衆国　94610　カルフォルニア州　オークランド　リーストリート　264　スイート102
(74)代理人　100099461
弁理士　溝井　章司

最終頁に続く

(54)【発明の名称】　情報管理システム及び情報管理方法及びシステム制御装置

(57)【要約】
【課題】　イントラネットとインターネット間の情報伝達はファイアウォール等を設けたハイレベルのセキュリティを有するシステムを通過できず、イントラネットの内外からシームレスに情報をアクセスできる情報管理システムを構築できなかった。
【解決手段】　イントラネット３０上にグループウエア情報とファイル管理のためのシステム制御装置６０を備え、インターネット１０上にはサービスサイト７０を備え、各クライアント４０，４１にファイル複製デーモン６３ｃを備えた。ファイル複製デーモン６３ｃは、システム制御装置６０と協調してクライアント４０上のデータをイントラネット上あるいはインターネット上のディスクリソース５０，６１，７１にファイル転送する。また、システム制御装置６０は、サービスサイト７０と協調してグループウエア情報の同期を取る。こうして、イントラネットの内外からシームレスに情報をアクセスすることができる。



【特許請求の範囲】
【請求項１】　アクセス端末を接続するインターネットと、
ファイアウォールを介してインターネットに接続され、クライアントを接続したイントラネットとを有するネットワークシステムの情報管理システムにおいて、
イントラネットに接続され、イントラネットに接続されたクライアントによりアクセスされるデータをマスタデータとして記憶するとともに、マスタデータをイントラネットからインターネットに対して転送するシステム制御装置と、
インターネットに接続され、システム制御装置から転送されたデータを受信して受信したデータをマスタデータの複製データとして記憶し、記憶した複製データをインターネットに接続されるアクセス端末からアクセスさせるサービスサイトとを備えたことを特徴とする情報管理システム。
【請求項２】　上記システム制御装置は、クライアントによるマスタデータの更新を監視し、サービスサイトの複製データに対してマスタデータと同一の更新を行うとともに、アクセス端末による複製データの更新を監視し、システム制御装置のマスタデータに対して複製データと同一の更新を行う情報更新デーモンを備えたことを特徴とする請求項１記載の情報管理システム。
【請求項３】　上記システム制御装置は、マスタデータとして複数の個人情報を記憶し、複数の個人情報からグループ情報を生成するイントラネットグループウエア情報管理部を備え、
上記サービスサイトは、上記複数の個人情報を受信して複製データとして記憶し、複数の個人情報からグループ情報を生成するインターネットグループウエア情報管理部を備えたことを特徴とする請求項１記載の情報管理システム。
【請求項４】　上記情報管理システムは、更に、クライアントにおいて動作し、クライアントからサービスサイトへデータを転送するファイル複製デーモンを有し、
上記システム制御装置は、複製データをサービスサイトに転送する条件をファイル複製ポリシーとして記憶し、ファイル複製ポリシーに基づいてクライアントが所有しているファイルをサービスサイトに転送するようにファイル複製デーモンに指示することを特徴とする請求項１記載の情報管理システム。
【請求項５】　上記システム制御装置は、アクセス端末又はクライアントからサービスサイトの複製データを選択させて、選択されたサービスサイトの複製データをアクセス端末又はクライアントへダウンロードするファイル制御部を備えたことを特徴とする請求項４記載の情報管理システム。
【請求項６】　アクセス端末を接続するインターネットと、
ファイアウォールを介してインターネットに接続され、クライアントを接続したイントラネットとを有するネットワークシステムにおける情報管理方法において、
イントラネットに接続されたクライアントによりアクセスされるデータをマスタデータとして記憶するとともに、マスタデータをイントラネットからインターネットに対して転送するシステム制御工程と、
システム制御工程により転送されたデータを受信して受信したデータをマスタデータの複製データとして記憶し、記憶した複製データをインターネットに接続されるアクセス端末からアクセスさせるサービスサイト工程とを備えたことを特徴とする情報管理方法。
【請求項７】　アクセス端末を接続するインターネットと、
インターネットに接続され、データを記憶し、記憶したデータをインターネットに接続されるアクセス端末からアクセスさせるサービスサイトとファイアウォールを介してインターネットに接続され、クライアントを接続したイントラネットとを有するネットワークシステムのイントラネットに接続されたシステム制御装置において、
イントラネットに接続されたクライアントによりアクセスされるデータをマスタデータとして記憶する記憶部と、
マスタデータをイントラネットからインターネットのサービスサイトに対して転送して、複製データとしてサービスサイトに記憶させる情報管理部と、
クライアントによるマスタデータの更新を監視し、サービスサイトの複製データに対してマスタデータと同一の更新を行うとともに、アクセス端末による複製データの更新を監視し、システム制御装置のマスタデータに対して複製データと同一の更新を行う情報更新デーモンとを備えたことを特徴とするシステム制御装置。
【請求項８】　上記サービスサイトは、アクセス端末からデータアクセス要求がある場合に、データアクセス要求のあったマスタデータをシステム制御装置から複製データとして複製してきて一時的に記憶するとともに、アクセス端末からのデータアクセス要求の消滅により複製データを消去することを特徴とする請求項１記載の情報管理システム。
【請求項９】　上記サービスサイトは、アクセス端末が生成したマスタデータに対する入出力コマンドをシステム制御装置に対して転送し、
システム制御装置は、サービスサイトから転送された入出力コマンドをマスタデータに対して実行することを特徴とする請求項１記載の情報管理システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、グループウエア機能とファイル共有機能を有するイントラネットとファイアウォールを介して接続してなるインターネット等エク

ストラネット構成において、特にイントラネットのセキュリティ性能を損なうことなく、それぞれのデータの整合性管理とデータの転送を効率的に行うのに好適な情報管理システムに関するものである。

【０００２】

【従来の技術】特定の企業間で秘匿性の高い情報を安全に共有するには、不正アクセスを防止するセキュリティシステムを構築することが不可欠である。例えば、イントラネット内に不正に外部からアクセスされることを防ぐために、ファイアウォールと呼ばれるゲートウエイを各イントラネットの入り口に配置している。

【０００３】しかし、このような構成では、各企業のそれぞれのイントラネット内にあるグループウエア上の情報や共有したいファイルの参照がファイアウォールによって阻止される。このような問題に対処するために、従来は、図９に示す技術が用いられている。

【０００４】図９は、イントラネット上のデータを外部からアクセスする場合の従来のシステムを示すブロック図である。図９において、１０はインターネット、１００はＡ社ネットワーク上のイントラネット、２０はファイアウォールである。同様に、３１はＢ社ネットワーク上のイントラネット、２１はファイアウォールで各社のイントラネットを外部からの進入から保護している。４０～４４はクライアントである。

【０００５】しかし、このような場合、Ａ社、Ｂ社間の情報のやりとり、ファイルのやり取りをインターネット１０を通じて行おうとしてもファイアウォール２０又は２１に阻止される。このような場合、両者は、ＶＰＮ（仮想私設網）接続を行っている。Ａ社ネットワーク１００上にＶＰＮサーバ１０２、Ｂ社ネットワーク上にＡ社のＶＰＮサーバと互換性のある別のＶＰＮサーバ２０１を設置して転送するデータを暗号化しＶＰＮトンネル１１を経由してデータを転送することによってセキュリティを確保している。

【０００６】更に、ファイアウォール２０にＲＡＳ（リモートアクセスサーバ）１０１を設け、そこに接続されているモデム１０３を介して外部の携帯端末８０からダイアルアップして情報やファイルを参照することも行われている。このような構成により、ファイアウォールを経由せずに、Ａ社ネットワーク１００のデータをアクセスできる。

【０００７】また、外部のＡＳＰ（アプリケーションサービスプロバイダ）３９０に業務をアウトソーシングし、Ａ社、Ｂ社あるいは外部から共有したい情報、ファイルを全てＡＳＰ３９０上のディスクリソース３９１上に格納、管理し使用参照する方法も行われている。このような構成によってインターネットを通じてどこからでも情報、ファイルを参照することができる。

【０００８】また、特開平１１－２１９３２６「電子ファイル管理システム」や、特開２０００－１４８６１１「イントラネットとデータベースサーバ及びそのデータ転送方法」に見られるように、情報やファイルを、例えば、電子メールの形に変換してイントラネット間の情報転送を行う方法等が考案されている。

【０００９】しかしながら、これらのような方法では、まず情報を暗号化するための装置を、情報を参照する場所全てに用意する必要が発生し、コストがかかり、更に、互換性の問題が発生する。また、ファイアウォールを経由しない経路を作る場合は、セキュリティが十分確保できない。更に、データを外部に置く場合は、外部記憶媒体へのアクセスに時間がかかり、また、ユーザからの負荷が集中するためにシステム自身の性能が悪化することがある。また、各種端末からのログインの手順が異なり使用方法が煩雑にり、更に、情報を外部に置くために秘匿性が守れない等の問題が発生し、当該シームレスなアクセスを実現化するに至っていない。

【００１０】なお、企業内ネットワーク、即ち、イントラネット３０を保護するためにインターネット１０との間に設けられたファイアウォール２０は、メール受信用にｐｏｐ３プロトコル（ポート番号１１０）、メール送信用にｓｍｔｐプロトコル（ポート番号２５）、ファイル転送用のｆｔｐプロトコル（ポート番号２１）又はＷｅｂ情報用のｈｔｔｐプロトコル（ポート番号８０）を利用して、なおかつ、メール以外のデータのアクセスは、イントラネットの内側から外側へのみを可能にしている。

【００１１】

【発明が解決しようとする課題】従来の技術では、企業内で使用している情報、ファイルがファイアウォール等を設けたハイレベルなセキュリティを有するネットワークを通過できない。

【００１２】本発明の目的は、現在使用されているセキュリティ技術を使用しつつも、シームレスなアクセスを可能とする情報管理システムを得るものである。

【００１３】

【課題を解決するための手段】この発明に係わる情報管理システムの好適な実施の形態は、ファイアウォールにてセキュアされたイントラネットと、このファイアウォールを介して当該イントラネットと通信を行うことができるインターネットとを有するネットワークシステムにおいて、イントラネット上に所属する各メンバに帰属するスケジュール等の個人情報とそのメンバが扱っているファイルを、マスタデータとして管理するシステム制御装置を備えるものである。

【００１４】この発明に係わる情報管理システムの好適な実施の形態は、イントラネットから利用できるディスクリソースと、そのディスクリソース上に上記イントラネット上の個人情報とファイルとを複製データとして格納する機能とを備えるサービスサイトをインターネット上に備えるものである。

【００１５】この発明に係わる情報管理システムの好適な実施の形態は、上記システム制御装置から上記サービスサイト上の個人情報と上記システム制御装置上の個人情報との両方の個人情報の変更を監視し、上記サービスサイト上の個人情報と上記システム制御装置上の個人情報を同一であるように上記サービスサイト上の個人情報と上記システム制御装置上の個人情報とを操作する個人情報更新デーモンを備えるものである。

【００１６】この発明に係わる情報管理システムの好適な実施の形態は、イントラネット上のクライアント上に、上記システム制御装置と連携を取りながら、クライアント上のマスタデータをイントラネットディスクリソース又は上記サービスサイトディスクリソースにマスタデータの複製データを転送するファイル複製デーモンを備えるものである。

【００１７】この発明に係わる情報管理システムの好適な実施の形態は、上記ファイル複製デーモンがマスタデータの複製データを生成するタイミングをファイル複製ポリシーにより設定可能である。更に、複製データの生成時には、ファイル名を変更し、ファイルを格納した時刻、格納を指示したクライアント名等のプロパティ情報を付加して転送するプロパティ付加部を備えるものである。

【００１８】この発明に係わる情報管理システムの好適な実施の形態は、イントラネットのクラアントからWWWブラウザで上記システム制御装置をアクセスすることによって、上記ファイル複製デーモンがイントラネットディスクリソースに格納した複製データを参照し、クライアントへダウンロードするイントラネットファイル情報管理部を備えるものである。

【００１９】この発明に係わる情報管理システムの好適な実施の形態は、インターネットのアクセス端末からからWWWブラウザで上記サービスサイトをアクセスすることによって、上記ファイル複製デーモンがイントラネットから転送したインターネット上のディスクリソースに格納した複製データを参照し、アクセス端末へダウンロードするインターネットファイル情報管理部を備えるものである。

【００２０】この発明に係わる情報管理システムの好適な実施の形態は、上記個人情報を利用してメンバが所属するグループのグループ情報を上記システム制御装置で生成するイントラネットグループ情報生成部と、同一のグループ情報を上記サービスサイトで生成するインターネットグループ情報生成部とを備えるものである。

【００２１】この発明に係わる情報管理システムの好適な実施の形態は、上記サービスサイト上の情報を、上記インターネット上に接続される各種のアクセス端末（クライアント、サービスプロバイダ経由の自宅のパソコン、携帯端末、携帯電話等）から、クライアントがユーザに提供しているユーザインタフェースと同一あるいは類似したユーザインタフェースで、かつ、ユーザがクライアントに対して入力するパスワードと同一のパスワードでアクセス可能な機能を備えるものである。

【００２２】上記サービスサイトは、アクセス端末からデータアクセス要求がある場合に、データアクセス要求のあったマスタデータをシステム制御装置から複製データとして複製してきて一時的に記憶するとともに、アクセス端末からのデータアクセス要求の消滅により複製データを消去することを特徴とする。

【００２３】上記サービスサイトは、アクセス端末が生成したマスタデータに対する入出力コマンドをシステム制御装置に対して転送し、システム制御装置は、サービスサイトから転送された入出力コマンドをマスタデータに対して実行することを特徴とする。

【００２４】

【発明の実施の形態】実施の形態１．以下、本発明の実施の形態を、図面により詳細に説明する。図１は、本発明によるイントラネットと他のネットワークとの接続を示すブロック図である。図１において、１０はインターネット、１００はＡ社ネットワーク、また、２００はＢ社ネットワークである。８０はノートパソコンや自宅のパソコンを含めた携帯端末、８１はそれら携帯端末８０を電話網経由でインターネット１０に接続するためのインターネットサービスプロバイダ、９０は携帯電話、９１はその携帯電話をインターネット１０に接続するための携帯電話インターネット接続網である。Ａ社ネットワーク１００とＢ社ネットワーク２００、更に、携帯端末８０、携帯電話９０はインターネット１０を通してお互いに接続されエクストラネットを構成している。

【００２５】Ａ社ネットワーク１００において、２０はファイアウォール、３０はイントラネット、４０，４１はイントラネット３０に接続されるクライアントである。Ｂ社ネットワーク２００において、２１はファイアウォール、３１はイントラネット、４３，４４はイントラネット３１に接続されるクライアントである。それぞれのイントラネットは、ファイアウォール２０又は２１によって外部からの攻撃に対して備えセキュリティを確保している。

【００２６】Ａ社ネットワーク１００において、５０はイントラネット３０上のクライアント間で共有することができるイントラネットディスクリソース、６０はグループウエアとファイルを管理するシステム制御装置、６１はシステム制御装置６０内にあって、イントラネットディスクリソース５０と同様に、各クラアントから共有できるイントラネットディスクリソース、６２はイントラネット３０上の各ユーザのスケジュール情報、コンタクト情報等グループウエア情報を管理するイントラネットグループウエア情報管理部、６３はイントラネット３０上のクライアント上のファイル情報を管理するイントラネットファイル情報管理部である。また、Ｂ社ネット

ワーク２００において、６９はシステム制御装置６０と同じシステム制御装置である。

【００２７】クライアント４０において、４０ａはクライアント４０上データを格納するローカルディスクリソースで、６３ｃはローカルディスクリソース４０ａのデータをイントラネットディスクリソース５０やインターネットディスクリソース７１に複製を作る作業するファイル複製デーモンである。

【００２８】サービスサイト７０において、７１はインターネット上にあって、Ａ社ネットワーク１００やＢ社ネットワーク２００、携帯端末８０等からアクセスすることができるインターネットディスクリソース、７２はインターネット１０上でＡ社ネットワーク１００及びＢ社ネットワーク２００上の各ユーザのスケジュール情報、コンタクト情報等グループウエア情報を管理するインターネットグループウエア情報管理部、７３はインターネット１０上でＡ社ネットワーク１００及びＢ社ネットワーク２００上のクライアント上のファイル情報を管理するイントラネットファイル情報管理部である。

【００２９】次に、グループウエア関連の各データの所在、流れを概略説明する。グループウエア情報は、システム制御装置６０に管理されており、マスタデータは、イントラネットディスクリソース６１に存在する。データの参照、更新等の作業は、イントラネットグループウエア情報管理部６２によって行われる。同様のデータがインターネットグループウエア情報管理部７２によっても管理されており、データはインターネットディスクリソース７１上に存在する。

【００３０】次に、ファイル関連の各データの所在、流れを概略説明する。各クライアント上のデータは、例えば、クライアント４０のデータは、ローカルディスクリソース４０ａに存在する。ファイル複製デーモン６３ｃは、ローカルディスクリソース４０ａのデータを複製し圧縮して、イントラネットディスクリソース５０、又はイントラネットディスクリソース６１、インターネットディスクリソース７１にデータの圧縮複製を転送する。イントラネットディスクリソース６１に転送され記憶されたデータは、イントラネットファイル情報管理部６３を経由して、クライアント４１に転送することができ、クライアント４１でデータを復元利用することができる。

【００３１】以下、図２，図３を用いてユーザインタフェースについて説明する。図２，図３の四角枠は、画面表示を示している。３００はイントラネットホームページで各ユーザの入り口である。コンテンツは物理的にはシステム制御装置６０にあり、各ユーザはイントラネット３０に接続された任意のクライアントからWWWブラウザ経由でアクセスできる。３０１は各ユーザ個人に割り当てられたイントラネット個人情報ページで、イントラネットホームページ３００のログイン画面にユーザＩＤとパスワードを入力することによって、各ユーザ単位に管理されたイントラネット個人情報ページ３０１をアクセスすることができる。３０２は各ユーザ個人のグループウエア情報をアクセスするための個人情報表示画面で、掲示板や行き先表示、会議室の予約等が操作確認できる。３０３は各ユーザが所属しているグループのスケジュール等グループメンバ全体の情報をマージした情報を確認できる画面である。画面３０２，３０３は、イントラネットグループウエア情報管理部６２により作成変更されたグループウエア情報を表示するものである。

【００３２】また、３０４は各ユーザ個人のディスクリソースを管理するリソース管理ページで、３０５はクライアント上のファイルをイントラネットディスクリソース５０、６１やインターネットディスクリソース７１にファイルを転送して複製を作るタイミングや条件を設定するポリシー設定画面、３０６はイントラネットディスクリソース５０、６１やインターネットディスクリソース７１にあるファイルの複製を表示して選択し、それをクライアント上にダウンロードすることができるファイルブラウザ画面、３０７はファイルブラウザ画面３０６にて表示した各ファイルそれぞれを作成された日付、バージョン、編集したクライアントの名前等のプロパティを表示するファイルブラウザ子画面である。画面３０４，３０５，３０６，３０７は、イントラネットファイル情報管理部６３が管理しているファイルやデータを表示するものである。

【００３３】図２において、３２０はイントラネットを管理する管理者のための管理者用ページでここを経由して以下の各ページをアクセスできる。３２１はグループウエアに参加するメンバを登録したり、あるいは共有の情報を管理するグループウエア管理画面、３２２はイントラネット上の各端末やその上で動作するファイル複製デーモン６３ｃの動作状態等を管理するファイルリソース管理画面である。画面３２１は、イントラネットグループウエア情報管理部６２が管理者にのみ提供するものである。画面３２２は、イントラネットファイル情報管理部６３が管理者にのみ提供するものである。

【００３４】図３において、更に、３１０はインターネット１０上のサービスサイト７０にありインターネット上のアクセス端末からアクセスでき、イントラネットのクライアントに入力するユーザＩＤとパスワードと同一のユーザＩＤとパスワードとを入力するサービスサイトホームページで、３１１はその個人情報をアクセスできるインターネット個人ページであり、イントラネット個人情報ページ３０１に相当する情報をインターネットアクセスできるものである。３１２はインターネット上の個人情報表示画面で、３１３はインターネット上のグループ情報表示画面である。画面３１２，３１３は、インターネットグループウエア情報管理部７２により作成変更されたグループウエア情報を表示するものである。３

１４はインターネット上のリソース管理画面で、３１６はインターネットディスクリソース７１上にあるファイルの複製を表示して選択し、それをインターネット経由で接続された携帯端末８０等にダウンロードすることができるファイルブラウザ画面、３１７はファイルブラウザ画面３１６にて表示した各ファイルそれぞれを作成された日付、バージョン、編集したクライアントの名前等のプロパティを表示するファイルブラウザ子画面である。画面３１４，３１６，３１７，３１８は、インターネットファイル情報管理部７３が管理しているファイルやデータを表示するものである。

【００３５】図3において、３１８はサービスサイト７０上にあって、システム制御装置６０やファイル複製デーモン６３ｃ等の保守情報やアップグレード情報を提供すると同時に、ファイルリソース管理ページ３２２と連携して動作し、各サービスの課金情報等を管理するサービスページである。画面３１８は、サービスサイト７０が管理者にのみ提供するものである。

【００３６】図2と図3において、以下の画面は、同一又は類似の表示及び同一又は類似のユーザインタフェースを持っている。画面３００と画面３１０、画面３０１と画面３１１、画面３０２と画面３１２、画面３０３と画面３１３、画面３０４と画面３１４、画面３０６と画面３１６、画面３０７と画面３１７。こうして、ユーザは、クライアントからでもアクセス端末からでも、同一の又は類似のオペレーションで同一内容のデータにアクセスできる。

【００３７】以下、図4を用いてシステム制御装置６０とサービスサイト７０上の個人情報とグループ情報の提示に関る詳細を説明する。６１ａ，６１ｂ，６１ｃはシステム制御装置６０上のイントラネットディスクリソース６１上にある各ユーザメンバの個人情報を示すイントラネットグループウエア個人情報である。６１ｅはイントラネットグループウエア個人情報６１ａ，６１ｂ，６１ｃがマージされたものであり、各ユーザメンバが所属するグループの情報を示すイントラネットグループウエアグループ情報である。６２ａはイントラネットグループウエア情報管理部６２内の機能であり、イントラネットグループウエアグループ情報６１ｅを生成するイントラネットグループ情報生成部である。

【００３８】７１ａ，７１ｂ，７１ｃはサービスサイト７０上のインターネットディスクリソース７１上にある各ユーザメンバの個人情報を示すインターネットグループウエア個人情報である。７１ｅはインターネットグループウエア個人情報７１ａ，７１ｂ，７１ｃがマージされたものであり、各ユーザメンバが所属するグループの情報を示すインターネットグループウエアグループ情報である。７２ａはインターネットグループウエア情報管理部７２内の機能でありインターネットグループウエアグループ情報７１ｅを生成するインターネットグループ情報生成部である。

【００３９】イントラネット上の各ユーザは、イントラネット個人情報表示画面３０２を使用して個人スケジュールや行き先表示、Ｔｏ　Ｄｏ　Ｌｉｓｔ、アドレス帳等の業務で使用している情報をアクセスし更新することができる。これらの情報は、イントラネットグループウエア個人情報６１ａ，６１ｂ，６１ｃに記録されているものである。３０３は各自の個人情報を所属するグループ単位にマージした情報を表示して、同一グループの構成員達の所在や、スケジュール等を確認するために使用するイントラネットグループ情報表示画面である。これらの情報は、イントラネットグループウエアグループ情報６１ｅとして記録される。

【００４０】一方、インターネット上の携帯端末８０等のアクセス端末で情報をアクセスするユーザは、インターネット個人情報表示画面３１２を使用して個人スケジュールや行き先表示、Ｔｏ　Ｄｏ　Ｌｉｓｔ、アドレス帳等の業務で使用している情報をアクセスし更新することができる。これらの情報はインターネットグループウエア個人情報７１ａ，７１ｂ，７１ｃに記録されているものである。３１３は各自の個人情報を所属するグループ単位にマージした情報を表示して、同一グループ員達の所在や、スケジュール等を確認するために使用するインターネットグループ情報表示画面である。これらの情報は、インターネットグループウエアグループ情報７１ｅに記録されているものである。

【００４１】図5において、インターネットグループウエア個人情報７１ａを例にとって、データ構造を示したものである。他のインターネットグループウエア個人情報７１ｂ，７１ｃ及びイントラネットグループウエア個人情報６１ａ，６１ｂ，６１ｃも同じデータ構造を有している。グループウエア個人情報には、各ユーザが通常のディスクリソースと使用できるデータ領域とグループウエアの個人情報が記録される。更に、個人情報表示画面を通じて各クライアントや携帯端末等から入力された内容の変更分の情報が変更差分情報として記録される。

【００４２】システム制御装置６０上の個人情報とサービスサイト７０上における個人情報のデータ配置の詳細を説明する。図6は、サービスサイト７０上にあるインターネットディスクリソース７１でのデータの配置を図示したものである。イントラネット３０に属する個人情報データ、例えば、７１ａ，７１ｂ，７１ｃ等がエリア７１ｈに配置されており、グループＡ７１ｆやグループＢ７１ｇを構成している。例えば、グループＢ７１ｇの場合は、インターネットグループウエア個人情報７１ａを含むメンバ1－4で一つのグループを構成している。７１ｅは各個人情報から作られたグループＡ，Ｂ等のグループ情報をインターネットグループウエアグループ情報として格納するブロックである。

【００４３】イントラネット３０に配置されているシス

テム制御装置６０のイントラネットディスクリソース６１に、イントラネットグループウエア個人情報６１ａ，６１ｂ，６１ｃが図6と同じ形式でデータが配置されている。イントラネット３０に配置されているシステム制御装置６０の個人情報は、インターネットディスクリソース７１上の領域７１ｈに配置される。同様に、イントラネット３１に配置されているシステム制御装置６９の個人情報は、インターネットディスクリソース７１上の領域７１ｊに配置される。このようにして、複数のイントラネットの情報が一つのサービスサイトにて管理されている。

【００４４】図7を用いシステム制御装置６０上の個人情報とサービスサイト７０上の個人情報の同期に関る詳細を説明する。ここで、同期とは、データの同一性を意味する。即ち、同期とは、マスタデータと複製データとの一方が更新された場合、他方も更新して両者を同一内容のデータとすることをいう。図7で、上半分がサービスサイト７０で扱われているデータ、下半分がシステム制御装置６０で扱われているデータである。インターネットグループ情報生成部７２ａがインターネットグループウエア個人情報７１ａ，７１ｂの個人情報を使って、インターネットグループウエアグループ情報７１ｅを生成し、同様に、イントラネットグループ情報生成部６２ａがイントラネットグループウエア個人情報６１ａ，６１ｂの個人情報を使って、イントラネットグループウエアグループ情報６１ｅを生成する様子を示している。

【００４５】インターネットグループウエア個人情報の個人情報に対する変更、例えば、スケジュール等の変更が各クライアントや携帯端末から行われた場合は、個人情報が直接変更されずに、それぞれのグループウエア個人情報の変更差分情報に変更内容が記録される。それは、イントラネット上でも同様の扱いを受ける。ここで、変更とは、グループウエア個人情報の新規生成も含むものとする。例えば、新規メンバｎが追加された場合、新規メンバｎ用のイントラネットグループウエア個人情報６１ｎのための記憶領域が確保され、記憶すべき内容が変更内容としてグループウエア個人情報の変更差分情報に記録される。

【００４６】６２ｄはシステム制御装置６０上に存在する個人情報更新デーモンであり、一定期間毎に、各個人情報の変更差分情報を監視し、なんらかのアップデートがあった場合には、システム制御装置６０側の個人情報、図では、イントラネットグループウエア個人情報６１ｂの個人情報を変更する。そして、イントラネットグループウエア個人情報、図では、６１ｂの個人情報をサービスサイト７０に転送して、インターネットグループウエア個人情報、図では、７１ｂの個人情報に書き込む。逆に、個人情報更新デーモン６２ｄは、インターネットグループウエア個人情報７１ｂの各個人情報の変更差分情報を監視し、なんらかのアップデートがあった場合には、インターネットグループウエア個人情報７１ｂの個人情報を変更する。そして、イントラネットグループウエア個人情報６１ｂの個人情報も変更する。新規メンバの追加も、変更の方法と同様の方法で行われる。こうして、サービスサイト７０上とシステム制御装置６０上のグループウエア個人情報の同期を、イントラネット上のクライアントからの変更と、インターネット上の携帯端末等からの変更をお互いに競合することなく、取ることができる。

【００４７】以下、図8用いてクラアント上のデータの複製に関る詳細を説明する。ユーザは、イントラネットファイル情報管理部６３が提供するポリシー設定画面３０５からファイル複製条件を入力する。例えば、ファイル複製条件として、図８では、複製タイミングとして、ファイルＡを「毎日１７時００分」に複製することを指定している。このファイル複製条件は、ファイル複製ポリシーデータ６３ｂとしてイントラネット情報管理部６３に記録される。このファイル複製ポリシーデータ６３ｂに基づいて、ファイル複製デーモン６３ｃがローカルディスクリソース４０ａのデータの複製を作る。図８では、クライアント４１上のデータＡをスケジューラ６３ｃａがファイル複製ポリシーデータ６３ｂの複製タイミングに設定されている時刻（１７：００）に従って、データＢ及びデータＣを複製する。又は、複製タイミングが「ファイルの更新時」となっている場合は、ファイル監視部６３ｃｂがファイルの更新を検知して複製する。ここで、複製とは、ファイルＡの全てのデータをコピーするのではない。ファイルＡへの書き込みデータに対して日付、バージョン、クライアントマシン名といったプロパティをプロパティ付加部６３ｃｃによって追加されたデータが、イントラネットディスクリソース５０上のデータＢ及びインターネットディスクリソース７１上のデータＣとして転送され複製ができる。即ち、データＢ、データＣは、プロパティが付加された差分データである。もし、ファイルＡが新規に生成された場合は、ファイルＡの内容全体が差分データとなる。

【００４８】プロパティ付加部６３ｃｃが付加するプロパティは、例えば、以下のものがある。ファイル名を変更した場合、変更後のファイル名。ファイルを格納した時刻。格納したファイルのバージョン。ファイルの格納を指示したクライアントマシン名。更新データ、書き込みデータに対する日付。更新データ、書き込みデータのバージョン。データの更新、書き込みを行ったクライアントマシン名。

【００４９】以下、図8用いてファイル制御部６３ａ，７３ａにより提供されるクライアント４０及び携帯端末８０でのデータの復元に関る詳細を説明する。各ユーザメンバは、ファイルブラウザ画面３０６，３１６によって必要なファイルを選択し、更に、ファイルブラウザ子画面３０７，３１７によって選択したファイルの過去の

履歴から必要なファイルを、プロパティとして付加された日付、バージョン、クライアントマシン名等から選択してダウンロードすることができる。データＢ、データＣは、プロパティが付加された差分データであり、この差分データを用いてクライアント４０又は携帯端末８０にファイルＡを生成できる。或いは、これらの差分データをクライアント４０又は携帯端末８０のファイルＡのデータとをあわせることにより、更新されたファイルＡを提供することができる。図では、クライアント４０がデータＢを自分のローカルディスクリソースにデータＤとしてダウンロードした例を示している。また、インターネットディスクリソース７１上のデータＣを携帯端末８０上のローカルディスクリソース８０ａにデータＥとしてダウンロードした例を示している。また、クライアント４０は、データＣを自分のローカルディスクリソースにデータＤとしてダウンロードすることもできる。しかし、携帯端末８０は、ファイアウォール２０があるために、データＢをローカルディスクリソース８０ａにデータＥとしてダウンロードすることはできない。

【００５０】この実施の形態は、ファイアウォールがあるために、インターネット上のサービスサイト（サーバ）にあるデータのアクセスは、イントラネット内側から外側へのみしか行えず、インターネットからイントラネットの内側に対しては、データのアクセスができないというシステムを前提として、ユーザがイントラネットにアクセスできない環境下にある時でも、イントラネットにアクセスしているのと全く同じ状態を提供するものである。イントラネットのマスタデータを複製し、インターネットに設けられたサービスサイトにファイル転送することにより、マスタデータがイントラネット内にあり、複製データがインターネット上にあるという状態を作る。そして、ユーザがイントラネットのマスタデータをアクセスできないときは、インターネットに用意された複製データをアクセスする。こうして、ユーザがイントラネットにアクセスできない環境下にある時でも、イントラネットにアクセスしているのと全く同じ状態を提供することができる。また、マスタデータの更新があったときは、イントラネット内の情報更新デーモンによりインターネット上の複製データも更新される。逆に、インターネット上の複製データの更新があったときは、イントラネット内の情報更新デーモンによりマスタデータも更新される。情報更新デーモンは、イントラネットの内側から外側へのみのアクセスを用いてデータ更新の監視とデータ更新をする。従って、情報更新デーモンは、インターネットからイントラネットの内側に対してはアクセスできないという制約があっても動作できる。また、イントラネットからインターネットへのファイル転送は、ファイル複製デーモンにより行われるが、ファイル複製デーモンは、イントラネットの内側から外側へのみのアクセスを用いてファイル転送を行う。従って、ファイル複製デーモンは、インターネットからイントラネットの内側に対してはアクセスできないという制約があっても動作できる。また、インターネットからイントラネットへのファイル転送は、クライアントからインターネットへのアクセスにより行われるので、インターネットからイントラネットの内側に対してはアクセスできないという制約があっても動作できる。また、この実施の形態では、メール送受信用プロトコルを用いなくてもよいので、メール送受信用プロトコルの制約を受けない。

【００５１】なお、個人情報又はファイルは、グループウエア以外に商品データベースやメール等でもよい。ファイルの転送は、前回転送分の差分情報でもよい。また、転送時にウイルスチェック等の動作を組み合わせてもよい。インターネット上に転送されたデータを他のイントラネットから参照して、複数のイントラネット環境上にあるデータベース間のデータを同期させるために使用してもよい。また、前述した各部、各デーモンは、ソフトウエアプログラムで実現できる。前述した各部、各デーモンがプログラムとして実現される場合、プログラムは、ディスクリソース等の記憶部に記憶され、クライアントコンピュータやシステム制御装置やサービスサイト（サーバ）コンピュータのＣＰＵにより記憶部から読み出され実行される。また、ディスクリソースとして、磁気ディスク、光ディスク、その他のディスク装置を用いることができる。ディスクリソースではなくて、その他の不揮発性記憶装置（記憶部）を用いてもよい。

【００５２】以上、この実施の形態によれば、ファイアウォールにて外部から保護されたイントラネットの環境をなんら変更することなく、必要なデータだけをインターネット上のパスワード等で保護されたサービスサイトに置き、インターネット上に接続された他ネットワーク上のクライアント、ダイアルアップした携帯端末、携帯電話などのアクセス端末から自由に情報をアクセスできる。

【００５３】例えば、Ａ社の社員である山田氏が社内に設置されたクライアント４０を使用して、パスワード「ＸＹＺ」を用いてローカルディスクリソース４０ａのファイルをアクセスしたり、イントラネットディスクリソース６１のイントラネットグループウエア個人情報６１ａとイントラネットグループウエアグループ情報６１ｅとをアクセスできる場合、山田氏が出張先のホテルからノートブックパソコン等の携帯端末８０から同一のパスワード「ＸＹＺ」を用いてサービスサイト７０のインターネットディスクリソース７１のファイルをアクセスしたり、インターネットグループウエア個人情報７１ａとインターネットグループウエアグループ情報７１ｅをアクセスすることにより、山田氏は、社外にいても社内でアクセスするマスタデータと同一の内容の複製データをアクセスできる。

【００５４】また、この実施の形態によれば、一つのシ

ステム制御装置で各メンバがアクセスするグループウエアの情報とファイルとの管理を同時にできるとともに、プロパティ付加部により複製データにプロパティが付加されているので、過去のファイル情報や他の環境から操作したファイルの情報をバックデートして参照することができる。

【００５５】また、この実施の形態によれば、マスタデータは全てイントラネット上に保全され、また、データの転送は、全てイントラネットのシステム制御装置から又はクライアントから又はアクセス端末から行われることにより、データの移動動作の負荷は分散され、サービスサイトのサーバに集中することがなく、本来の業務のレスポンス低下を防ぐことができ、更に、複数のシステム制御装置をサービスサイト経由で連携させて動作させることができるので、システムの規模に応じたスケーラビリティを確保することができる。

【００５６】また、この実施の形態によれば、各ファイルをイントラネットあるいはインターネット上のディスクリソースに重複して分散配置し、なおかつ、マスタファイルは、イントラネット上にあるので、ファイルの保全性を高められると同時に、社外のネットワーク障害等に対する耐障害性を確保することができる。

【００５７】実施の形態２．実施の形態１では、サービスサイト７０にＡ社のマスタデータの複製データを常時置くことになっているが、サービスサイト７０には複製データを常時置かずに、携帯端末８０又は携帯電話９０がサービスサイト７０を経由してＡ社ネットワーク１００のシステム制御装置６０に記憶されたデータをアクセスできるようにしてもよい。サービスサイト７０を経由してＡ社ネットワーク１００のシステム制御装置６０に記憶されたデータをアクセスする場合は、複製データはサービスサイト７０に滞留しない。即ち、上記サービスサイト７０に記憶されるファイルは、ディスク上の一時ファイル、又は、メモリ上のキャッシュファイルで良い。上記サービスサイト７０に記憶されるファイルは、一時的な（瞬時的な）ものなので、この方式は、携帯端末８０又は携帯電話９０がサービスサイト７０を経由してＡ社ネットワーク１００のシステム制御装置６０に記憶されたデータを透過アクセスできることを意味する。

【００５８】この場合は、複製データはサービスサイト７０に滞留しない（サービスサイト７０を透過する）ので社外にデータ保持されず、ユーザのクリティカルなデータが企業内のファイルサーバのみにに集中管理され、セキュリティの向上が図れる。以下、ディスク上の一時ファイルを用いて、携帯端末８０又は携帯電話９０がサービスサイト７０を経由してＡ社ネットワーク１００のシステム制御装置６０に記憶されたデータを透過的にアクセスする場合について説明する。

【００５９】１．Ａ社ネットワーク１００のシステム制御装置６０はサービスサイト７０に対してコネクションを確立して（或いは、ポーリングをして）、Ａ社ネットワーク１００の外部からのアクセスに備える。

２．携帯端末８０又は携帯電話９０はサービスサイト７０に対してデータの転送を要求する。

３．データの転送要求を受信したサービスサイト７０は、システム制御装置６０に対して、携帯端末８０又は携帯電話９０からのデータの転送要求の内容を伝える。

４．携帯端末８０又は携帯電話９０からのデータの転送要求の内容に基づき、システム制御装置６０は、マスタデータのなかから要求されたデータのみをサービスサイト７０に対して転送する。

５．上記サービスサイト７０のインターネットディスクリソース７１は、システム制御装置６０から転送されたデータを受け取り、受け取ったデータをディスク上の一時ファイルとして記憶する。

６．携帯端末８０又は携帯電話９０は、サービスサイト７０のインターネットディスクリソース７１にディスク上の一時ファイルとして一時的に記憶されたデータを自分に転送する。

７．携帯端末８０又は携帯電話９０ての転送が完了した時点でサービスサイト７０は、インターネットディスクリソース７１のディスク上の一時ファイルを消去する。

【００６０】次に、キャッシュファイルを用いて、携帯端末８０又は携帯電話９０がサービスサイト７０を経由してＡ社ネットワーク１００のシステム制御装置６０に記憶されたデータを透過的にアクセスする場合について説明する。

１．サービスサイト７０には、インターネットディスクリソース７１の代わりに（或いは、インターネットディスクリソース７１とともに）、サービスサイト７０の外部からのアクセスを高速にする目的でキャッシュメモリ（図示せず）を予め置く。

２．携帯端末８０又は携帯電話９０はサービスサイト７０に対してデータの転送を要求する。

３．データの転送要求を受信したサービスサイト７０は、携帯端末８０又は携帯電話９０が転送要求しているデータファイルがキャッシュメモリに有るか否かをチェックし、そのデータファイルがキャッシュメモリに有れば、そのデータファイルをキャッシュメモリから取得して携帯端末８０又は携帯電話９０に送信する。そのデータファイルがキャッシュメモリにない場合は、サービスサイト７０は、システム制御装置６０に対して、携帯端末８０又は携帯電話９０からのデータの転送要求の内容を伝える。

４．携帯端末８０又は携帯電話９０からのデータの転送要求の内容に基づき、システム制御装置６０は、要求されたデータをサービスサイト７０に対して転送する。

５．上記サービスサイト７０のインターネットディスクリソース７１は、システム制御装置６０から転送されたデータを受け取り、受け取ったデータをキャッシュファ

イルとして記憶する。すでにキャッシュメモリが他のデータファイルで占有されており空き領域がない場合には、ＬＲＵ（ｌｅａｓｔ　ｒｅｃｅｎｔｌｙ　ｕｓｅｄ）等の公知のアルゴリズムを用いてキャッシュメモリのデータファイルの内容が新たなデータファイルの内容で上書きされる。

６．携帯端末８０又は携帯電話９０は、サービスサイト７０のキャッシュファイルとして一時的に記憶されたデータを自分に転送する。

【００６１】以上のようなシステムでは、膨大なディスクリソース等を持ち保守するリスクは発生しない。即ち、複製データを一時ファイル、又は、キャッシュファイルにして、複製データを消すようにしたので、大容量の記憶装置がいらなくなる。

【００６２】ここで、システム制御装置６０をＡ社、Ｂ社等のユーザに販売し、さらに、サービスサイト７０を運営して、毎月Ａ社、Ｂ社等のユーザから、サービスサイト７０への接続料を徴収している会社を、以下、「サービス提供者」と呼ぶことにする。上記システムを、「サービス提供者」の立場からみた場合、Ａ社、Ｂ社等のユーザは、インターネット上のサービスサイト７０をゲートウエイとしてアクセスするので、Ａ社、Ｂ社等のユーザの各部門、各支店、各工場の各インターネット接続をサービスサイト７０に束ねることができる。上記システムでは、Ａ社、Ｂ社等の各ユーザの社員は、社外、各部門、各支店、各工場にいて自分の社内にある情報をアクセスする場合、携帯端末８０又は携帯電話９０を用いて、サービス提供者のサービスサイト７０に一旦接続することにより、自分の社内にある情報を自由にアクセスすることができる。社外、各部門、各支店、各工場にいる社員は、社内のデータをアクセスするために、サービス提供者のサービスサイト７０に接続しないといけないので、サービス提供者は、サービスサイト７０を経由して、ユーザに対して、情報検索、情報整理、情報提供等の新しいビジネスモデルを提供することができる。例えば、サービス提供者は、サービスサイト７０から、ユーザの社員にお知らせを一斉同報したり、ユーザの社内情報を一括して吸い上げたりというサービスを各ユーザごとに提供することができるようになる。

【００６３】また、例えば、Ａ社のＸ工場でシステム制御装置６０が採用されて実施の形態１又は２で述べたシステムがＡ社のＸ工場に所属する社員に適用され、次に、Ａ社のＹ工場でシステム制御装置６０が採用されて実施の形態１又は２で述べたシステムがＡ社のＹ工場に所属する社員に適用され、さらに、Ａ社の本社でシステム制御装置６０が採用されて実施の形態１又は２で述べたシステムがＡ社の本社に所属する社員に適用されるというように、順次このシステムが使われるようになった後、サービスサイト７０にＡ社がＡ社ポータルサイトを作れば全社ポータルサイトが完成する。このように、最初は、会社の一部の組織で利用されていたシステムが最後は会社全体で利用されるようになり、サービス提供者は、会社の一部の組織から会社全体を相手にビジネスができるようになる。

【００６４】実施の形態３．前述した実施の形態１，２では、転送する内容は主にデータ（例えば、ファイルされたデータ又はスケジュールデータ）であるが、転送する内容を、データそのものではなく、入出力（インプットアウトプット：ＩＯ）コマンド、例えば、ＳＣＳＩ（スモールコンピュータシステムインタフェース）でアクセスされるディスク装置に対するリードコマンド及びライトコマンドにしてもよい。

【００６５】例えば、携帯端末８０がシステム制御装置６０のイントラネットディスクリソース６１に対して”ファイル”を送るのではなく、イントラネットディスクリソース６１のディスクＩＯコマンドを直接送るようにする。

【００６６】ここで用いられるディスクＩＯコマンドは、例えば、ディスク装置をブロックアクセスデバイスとしてアクセスするコマンドである。携帯端末８０が転送するディスクＩＯコマンド（ディスクリードコマンド又はディスクライトコマンド）は、システム制御装置６０で動作しているＯＳ（オペレーティングシステム）がイントラネットディスクリソース６１をリード・ライトするときのコマンドと同じもの（同じコマンドフォーマットでかつ同じパラメータ）でなければいけない。イントラネットディスクリソース６１がＳＣＳＩを用いて接続されている場合には、一般的には公知のＳＣＳＩコマンドをそのまま使用することができる。

【００６７】ディスクＩＯコマンドを直接送る手順はデータの転送の場合と同様である。一例として、以下に、携帯端末８０がシステム制御装置６０のイントラネットディスクリソース６１に対してディスクリードコマンドを直接送ってマスタデータを読み取る手順を説明する。

【００６８】１．システム制御装置６０がサービスサイト７０に対してコネクションを確立する。

２．携帯端末８０はサービスサイト７０に対してディスクリードコマンドの転送要求を出す。

３．サービスサイト７０は、携帯端末８０からディスクリードコマンドを受信し、システム制御装置６０に転送する。

４．システム制御装置６０はサービスサイト７０からディスクリードコマンドを受け取り、イントラネットディスクリソース６１に対してディスクリードコマンドを実行する。

５．システム制御装置６０は、リードしたデータをサービスサイト７０に対して転送する。

６．サービスサイト７０はデータをさらに要求もとの携帯端末８０に対して送る。

以上がディスクリードコマンドの転送によるリード処理

の手順である。

【００６９】次に、携帯端末８０からディスクライトコマンドを用いてシステム制御装置６０のイントラネットディスクリソース６１にデータを書き込む場合の手順を以下に説明する。

【００７０】１．システム制御装置６０がサービスサイト７０に対してコネクションを確立する。

２．携帯端末８０はサービスサイト７０に対してディスクライトコマンドと書き込みデータとが発生したことを通知する。

３．サービスサイト７０は、携帯端末８０からの通知を受信し、システム制御装置６０に転送する。

４．システム制御装置６０は、サービスサイト７０から通知を受け取り、ディスクライトコマンドと書き込みデータとが携帯端末８０に有ることを知る。

５．システム制御装置６０は、ディスクライトコマンドと書き込みデータとをサービスサイト７０経由で（或いはインターネット１０経由で）能動的に携帯端末８０に取得しに行く。

６．システム制御装置６０は、取得したディスクライトコマンドと書き込みデータとを用いて書き込み処理を実行する。

以上がディスクライトコマンドの転送によるライト処理の手順である。

【００７１】以上のように、サービスサイト７０は、携帯端末８０が生成したマスタデータに対する入出力コマンドをシステム制御装置６０に対して転送する。また、システム制御装置６０は、サービスサイト７０から転送された入出力コマンドをマスタデータに対して実行する。したがって、携帯端末８０からシステム制御装置６０に対してデータの読み書きを指示することができ、データそのものを転送する場合に比べて、より柔軟性のあるシステムとなる。

【図面の簡単な説明】

【図１】　本発明の全体システムの一実施の形態を示すブロック図である。

【図２】　図１におけるイントラネットでのユーザインタフェースの関係を示すブロック図である。

【図３】　図１におけるインターネットでのユーザインタフェースの関係を示すブロック図である。

【図４】　図１におけるグループウエア情報管理部の処理動作を示すブロック図である。

【図５】　図４におけるデータブロックのフォーマットを示す図である。

【図６】　図１におけるディスクリソース上のデータの配置を示すブロック図である。

【図７】　図６におけるデータブロックの処理を示すブロック図である。

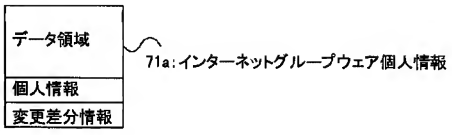
【図８】　図１におけるファイル情報管理部に係わるデータの操作を示すブロック図である。

【図９】　従来のシステムを示すブロック図である。

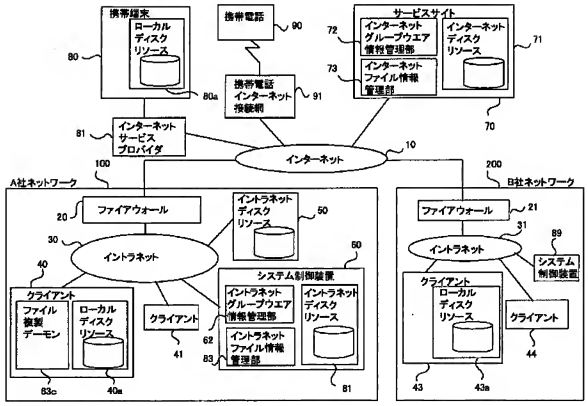
【符号の説明】

１０　インターネット、２０　ファイアウォール、２１　ファイアウォール、３０　Ａ社イントラネット、３１　Ｂ社イントラネット、４０　クライアント、４１－４４　クライアント、６０　システム制御装置、６１　イントラネットディスクリソース、６２　イントラネットグループウエア情報管理部、６３　イントラネットファイル情報管理部、７０　サービスサイト、７１　インターネットディスクリソース、７２　インターネットグループウエア情報管理部、７３　インターネットファイル情報管理部、８０　携帯端末、８１　インターネットサービスプロバイダ、９０　携帯電話、９１　携帯電話インターネット接続網、１００　Ａ社ネットワーク、２００　Ｂ社ネットワーク。

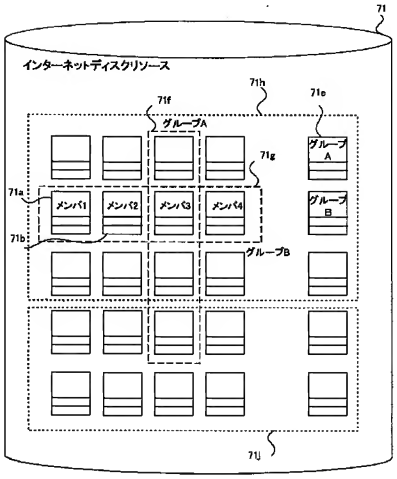
【図５】



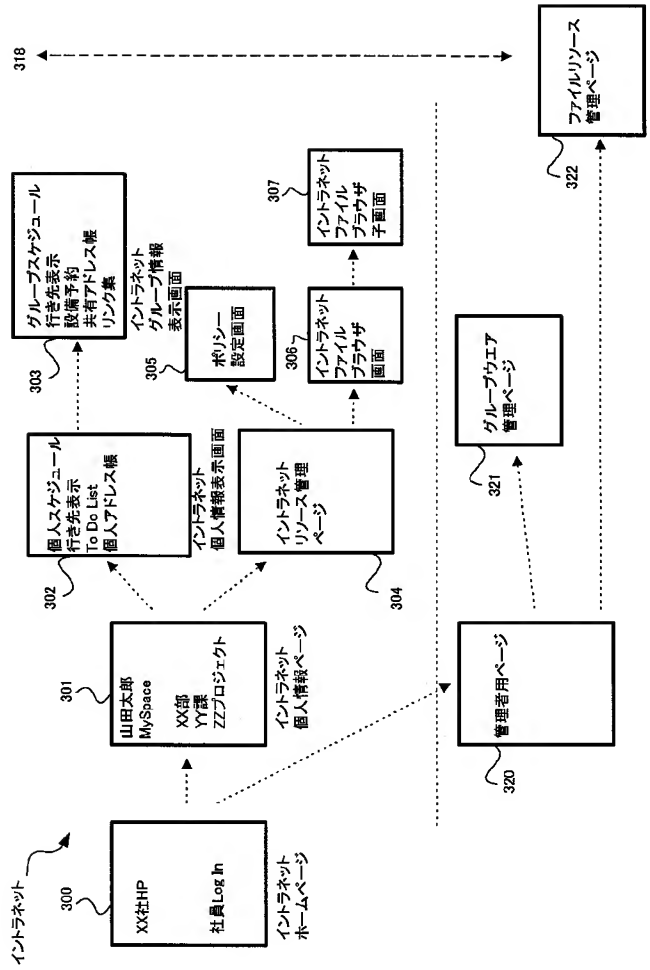
【図１】


携帯端末
ローカル
ディスク
リソース
80
80a
携帯電話
90
携帯電話
インターネット
接続網
91
サービスサイト
インターネット
グループウエア
情報管理部
72
インターネット
ディスク
リソース
71
インターネット
ファイル情報
管理部
73
70
インターネット
サービス
プロバイダ
81
インターネット
10
100
200
A社ネットワーク
B社ネットワーク
ファイアウォール
20
イントラネット
ディスク
リソース
50
イントラネット
30
システム制御装置
40
クライアント
ファイル
複製
デーモン
ローカル
ディスク
リソース
クライアント
41
イントラネット
グループウエア
情報管理部
62
イントラネット
ディスク
リソース
イントラネット
ファイル情報
管理部
83
83c
40a
81
ファイアウォール
21
31
イントラネット
89
システム
制御装置
クライアント
ローカル
ディスク
リソース
クライアント
44
43
43a

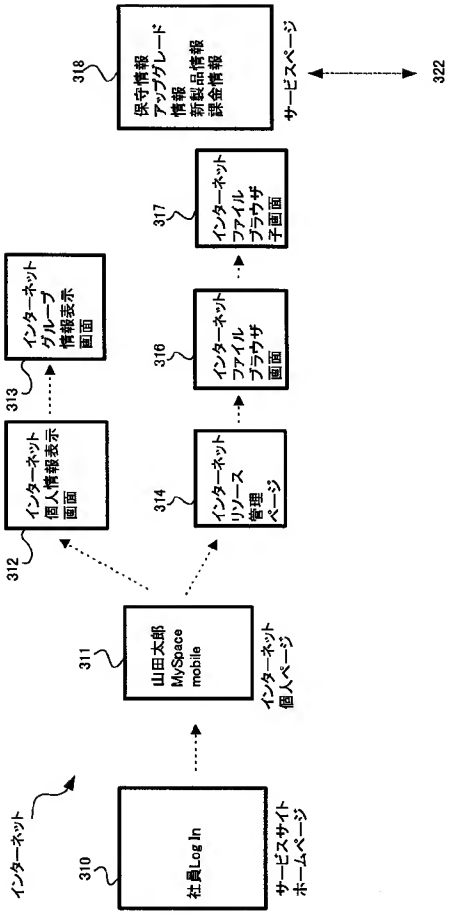
【図６】


71
インターネットディスクリソース
71h
71e
71f
グループA
グループ
A
71g
71a
メンバ1
メンバ2
メンバ3
メンバ4
グループ
B
71b
グループB
71j

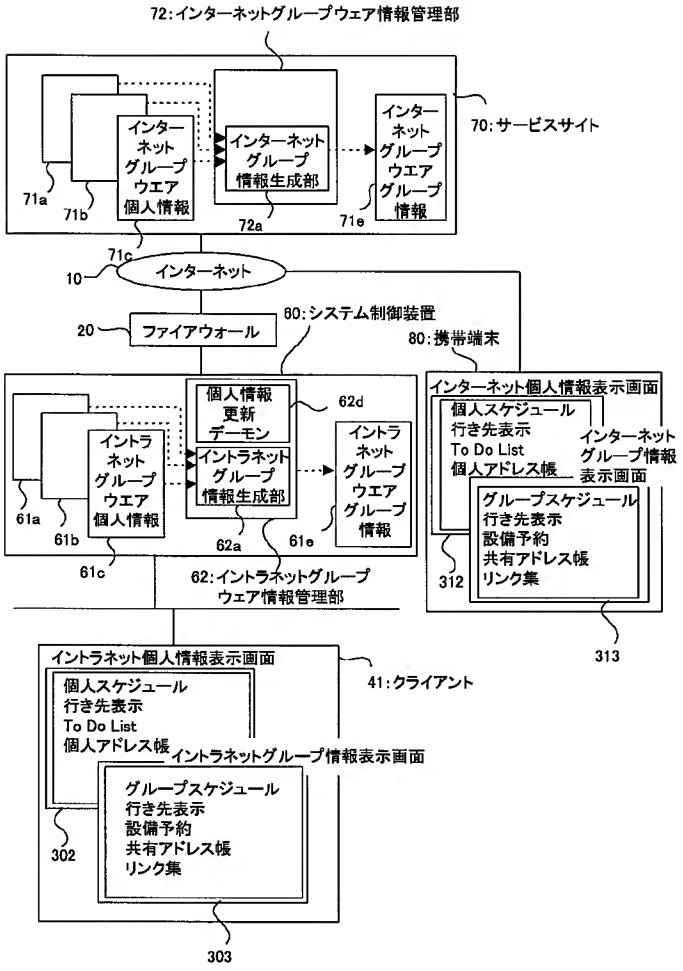
【図2】


イントラネット
300
XX社HP
社員Log In
イントラネット
ホームページ
301
山田太郎
MySpace
XX部
YY課
ZZプロジェクト
イントラネット
個人情報ページ
302
個人スケジュール
行き先表示
To Do List
個人アドレス帳
303
グループスケジュール
行き先表示
設備予約
共有アドレス帳
リンク集
イントラネット
個人情報表示画面
イントラネット
グループ情報
表示画面
304
イントラネット
リソース管理
ページ
305
ポリシー
設定画面
306
イントラネット
ファイル
ブラウザ
画面
307
イントラネット
ファイル
ブラウザ
子画面
318
320
管理者用ページ
321
グループウエア
管理ページ
322
ファイルリソース
管理ページ

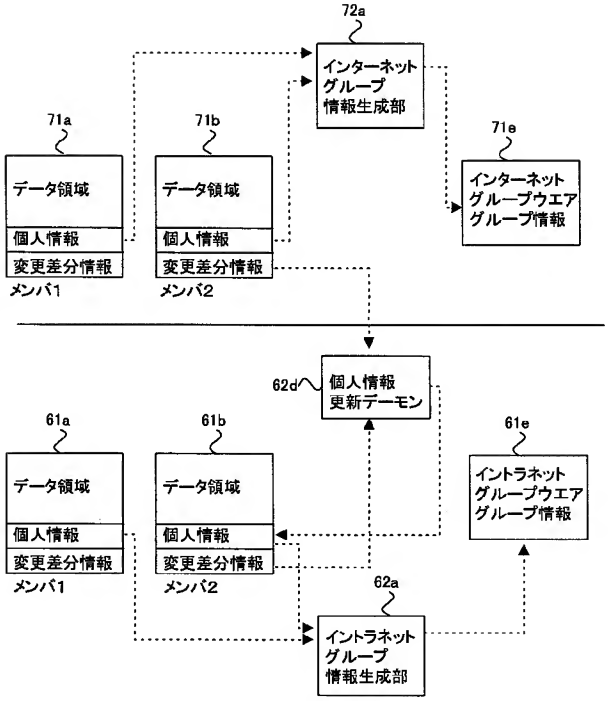
【図3】


インターネット
310
社員Log In
サービスサイト
ホームページ
311
山田太郎
MySpace
mobile
インターネット
個人ページ
312
インターネット
個人情報表示
画面
313
インターネット
グループ
情報表示
画面
314
インターネット
リソース
管理
ページ
316
インターネット
ファイル
ブラウザ
画面
317
インターネット
ファイル
ブラウザ
子画面
318
保守情報
アップグレード
情報
新製品情報
課金情報
サービスページ
322

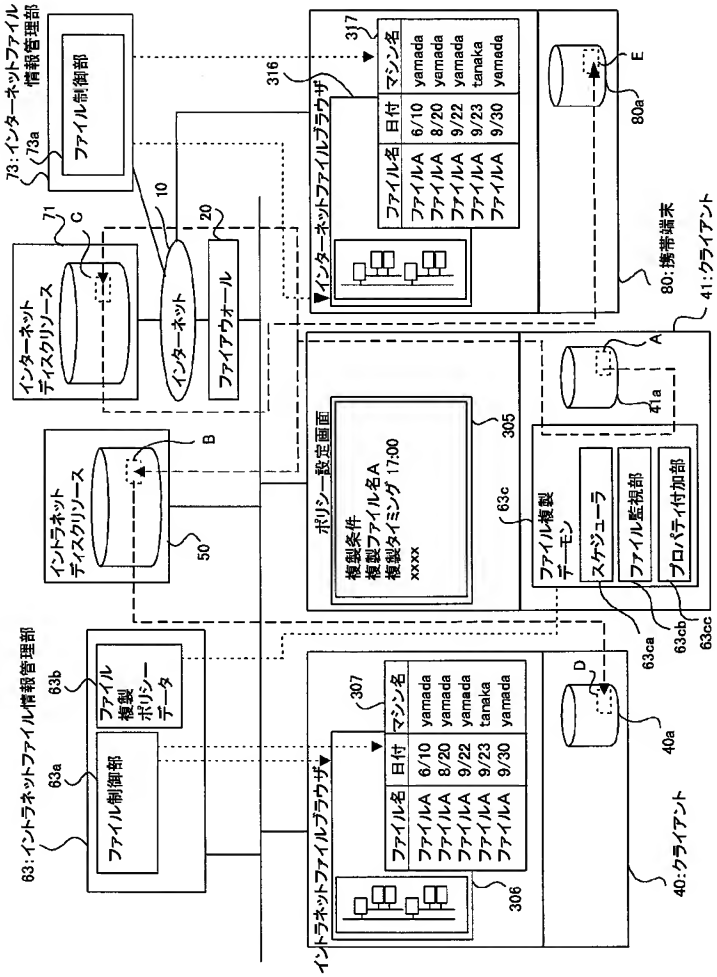
【図４】


72:インターネットグループウェア情報管理部
70:サービスサイト
インターネットグループウエア個人情報
インターネットグループ情報生成部
インターネットグループウエアグループ情報
71a
71b
72a
71e
71c
10
インターネット
20
ファイアウォール
80:システム制御装置
80:携帯端末
個人情報更新デーモン
62d
イントラネットグループ情報生成部
イントラネットグループウエア個人情報
イントラネットグループウエアグループ情報
61a
61b
61c
62a
61e
62:イントラネットグループウェア情報管理部
インターネット個人情報表示画面
個人スケジュール
行き先表示
To Do List
個人アドレス帳
インターネットグループ情報表示画面
グループスケジュール
行き先表示
設備予約
共有アドレス帳
リンク集
312
313
イントラネット個人情報表示画面
41:クライアント
イントラネットグループ情報表示画面
302
303

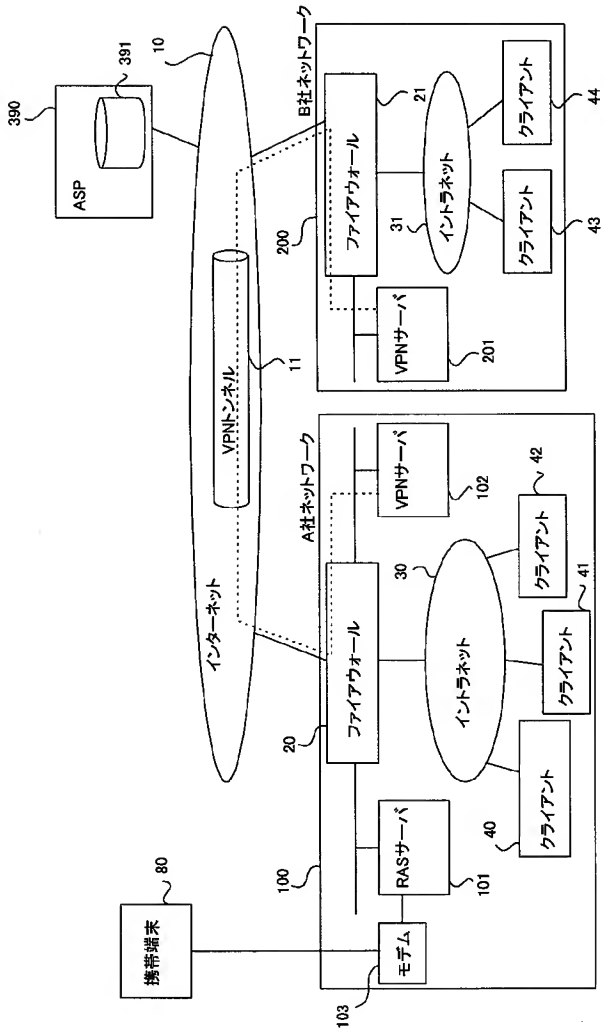
【図7】


72a
インターネット
グループ
情報生成部
71a
71b
71e
データ領域
個人情報
変更差分情報
メンバ1
データ領域
個人情報
変更差分情報
メンバ2
インターネット
グループウエア
グループ情報
62d
個人情報
更新デーモン
61a
61b
61e
データ領域
個人情報
変更差分情報
メンバ1
データ領域
個人情報
変更差分情報
メンバ2
イントラネット
グループウエア
グループ情報
62a
イントラネット
グループ
情報生成部

【図8】


73:インターネットファイル情報管理部
73a
ファイル制御部
J1
C
10
20
インターネットディスクリソース
インターネット
ファイアウォール
316
317
インターネットファイルブラウザ
ファイル名 日付 マシン名
ファイルA 6/10 yamada
ファイルA 8/20 yamada
ファイルA 9/22 yamada
ファイルA 9/23 tanaka
ファイルA 9/30 yamada
80a
E
80:携帯端末
41:クライアント
A
41a
イントラネットディスクリソース
B
50
ポリシー設定画面
複製条件
複製ファイル名A
複製タイミング 17:00
xxxx
305
63c
ファイル複製デーモン
スケジューラ
ファイル監視部
プロパティ付加部
63ca
63cb
63cc
63:イントラネットファイル情報管理部
63a
ファイル制御部
63b
ファイル複製ポリシーデータ
307
イントラネットファイルブラウザ
ファイル名 日付 マシン名
ファイルA 6/10 yamada
ファイルA 8/20 yamada
ファイルA 9/22 yamada
ファイルA 9/23 tanaka
ファイルA 9/30 yamada
306
D
40a
40:クライアント

【図9】


ASP
390
391
10
インターネット
VPNトンネル
11
B社ネットワーク
ファイアウォール
200
21
イントラネット
31
VPNサーバ
201
クライアント
44
クライアント
43
A社ネットワーク
ファイアウォール
20
30
イントラネット
VPNサーバ
102
クライアント
42
クライアント
41
クライアント
40
RASサーバ
101
100
モデム
103
携帯端末
80

フロントページの続き

Fターム(参考) 5B082 GB02 GB06 HA03
5B085 AA01 AE00
5B089 GA11 JA40 KA17 KB13